UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/565,567	01/23/2006	Jorge Abellan Sevilla	09669/081001	2117

22511 7590 10/29/2008

OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
4148	

NOTIFICATION DATE	DELIVERY MODE
10/29/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
buta@oshaliang.com

Office Action Summary	Application No.	Applicant(s)	
	10/565,567	SEVILLA, JORGE ABELLAN	
	Examiner	Art Unit	
	SIMON KANAAN	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/23/2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) *8* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9 and 10* is/are rejected.

7)☒ Claim(s) *1,5 and 8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/7/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10565567 filed on 1/23/2006 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63.**

Examiner Notes

3. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner

Priority

4. As required bye **M.P.E.P. 201.14(c)**, acknowledgement is made of applicant's claim for priority based on applications filed on July 23, 2003 (EPO 03291823) and October 29, 2003 (EPO 03292704).

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

5. The applicant's drawings submitted are acceptable for examination purposes.

Information Disclosure Statement

6. The information disclosure statement (IDS) submitted on 6/7/2006 has been acknowledged. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Objections

7. Claims 1, 5 and 8 are objected to because they refer to "tamper resistant module" which is a desired effect of a module and not a specific type of it.

8. Claim 8 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim cannot depend from any other multiple dependent claim. See MPEP § 608.01(n). Accordingly, the claim has not been further treated on the merits.

9. Claim 10 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim should refer to other claims in the alternative only. See MPEP § 608.01(n). Accordingly, the claim has not been further treated on the merits.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claim 10 is rejected under 35 U.S.C. 101 as directed o non-statutory subject matter of software, *per se*. The claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. It is at best, function descriptive material *per se*.

12. In this case, applicant has claimed a "computer program including program code instructions" for causing a computer to "execute" instructions in the preamble to these claims; this implies that Applicant is claiming a system of software, per se, lacking the hardware necessary to realize any of the underlying functionality. Therefore, claim 10 is directed to non-statutory subject matter as computer programs, per se, i.e. the

descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer, which permit the computer program's functionality to be realized.

Claim Rejections - 35 USC § 112

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claims 1 and 9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

15. As per claim 1 and 9, the limitation "counter is used to prove the amount of data flow" (line 14) renders this claim as vague and indefinite. It is not clear to the examiner whether how the counter proves the amount of data flow. Whether it is the number of times the data is encrypted hence data flow is the counter times the amount of data decrypted or if the counter is proving the amount of each data bit flow. It appears to the examiner that applicants refer to "counter is used to prove the amount of data flow" (line 14) as the counter along with the known size of data encrypted gives the total data flow.

Claim Rejections - 35 USC § 102

16. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

17. Claims 1, 2, 6, and 9 are rejected under 35 U.S.C. 102(b) as being anticipated by Andreaux et al. (WO 02/47365 A2)

As per claim 1, Andreaux discloses: "Method for monitoring the usage of a service by a communication device coupled to a tamper resistant module, in particular a smart card, *(page 9, lines 17 through 21, a smart card is used)* said service being transmitted from a resource able to communicate with said communication device by way of a network, *(page 1, lines 7 and 8, the digital data is transferred in a digital network)* "said service comprising a plurality of encrypted data flow, the use of said service comprising successive decryption steps of data flow by a respective first key EK, said first key EK being encrypted in the data flow" *(page 9, lines 17 through 21, smart card stores encrypted data as well as cryptographic keys, and page 8, lines 12 through 20, the information is decrypted multiple times)* "and decrypted in the tamper resistant module by way of a second key KEK stored in said tamper resistant module or derived inside said module," *(page 5, lines 33 through 36, a second key is used for encryption and decryption, and page 8, lines 12 through 20, the smart card stores cryptographic keys)* "characterized in that said method comprises the following steps:

a. A counting step, in which a memory location stores a count of occurrences of decryption steps of said first key EK attached to a same service; *(page 8, lines 12 through 20, the counter is decremented each time the key is used)*

b. A using step, in which said counter is used to prove the amount of data flow which has been decrypted." *(page 8, lines 12 through 20, the counter is decremented each time the key is used. The counter is used to verify number of times the content can be transmitted hence data flow)*

As per claim 2, Andreaux discloses: "Method according to claim 1, characterized in that the module stores a predetermined fixed number, and in that it comprises a comparison step in which the incrementing counter is compared to the predetermined fixed number for checking if the counter has reached or not the value of the fixed number; if yes, adequate action can be performed." *(page. 8, lines 12-20, counter is decremented, which is incrementing by -1, and compared to zero which is the predetermined fixed number. Action is performed until the counter equals zero)*

As per claim 6, Andreaux discloses: "Method according to claim 2, characterized in that the action is the completion of decryption steps." *(The data is encrypted and is transmitted a certain number of times with the key if the key is not equal to zero. This is part of the decryption steps.)*

As per claim 9, Andreaux discloses: "Data processing module, in particular a smartcard," *(page 9, lines 17 through 21, a smart card is used)* "able to receive services from a network," *(page 1, lines 7 and 8, the digital data is transferred in a digital network)* "said service comprising a plurality of encrypted data flow, the use of said service comprising successive decryption steps of data flow by a respective first key EK, said first key EK being encrypted in the data flow" *(page 9, lines 17 through 21, smart card stores encrypted data as well as cryptographic keys, and page 8, lines 12 through 20, the information is decrypted multiple times)* "and decrypted in said module by way of a second key KEK stored in said module or derived inside said module," *(page 5, lines 33 through 36, a second key is used for encryption and decryption, and page 8, lines 12 through 20, the smart card stores cryptographic keys)* "characterized in that module comprises a microcontroller able to perform he following steps:

a. A counting step, in which a memory location stores a count of occurrences of decryption steps of said first key EK attached to a same service; *(page 8, lines 12 through 20, the counter is decremented each time the key is used)*

b. A using step, in which said counter is used to prove the amount of data flow which has been decrypted." *(page 8, lines 12 through 20, the counter is decremented each time the key is used. The counter is used to verify number of times the content can be transmitted hence data flow)*

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 3, 4, 5, 7 and 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Andreaux in view of Maillard et al. (US 2002/0048367 A1).

As per claim 3, Andreaux discloses: "Method according to claim 1," but fails to disclose expressly "characterized in that a command is sent to the tamper resistant module for renewing the key KEK."

Maillard discloses "characterized in that a command is sent to the tamper resistant module for renewing the key KEK."*(page 4, paragraphs 58 and 59, describes a method including a command sent to the tamper resistant module for the renewing of the key)*

Andreaux and Maillard are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of sending a command to the tamper resistant module for renewing the KEK as described by Maillard with the method of monitoring the usage of service as taught by Andreaux because it would prevent the data from being reproduced *(Maillard, page 1, paragraph 9, lines 4 and 5)*

20. As per claim 7, Andreaux discloses: "Method according to claim 1," but fails to disclose expressly "characterized in that, each first key is sent periodically, and in that the amount of data is converted into time of use limiting the use of a service in time."

Maillard discloses "characterized in that, each first key is sent periodically," *(page 4, paragraph 58, lines 4 through 7, the encryption key changed monthly hence periodically)* "and in that the amount of data is converted into time of use limiting the use of a service in time." *(Maillard, page 1, paragraph 11, the key is updated periodically according to the subscription. When user terminates subscription they would not retrieve the new key in order to continue decrypting data. Hence the service is limited to time of subscription.)*

Andreaux and Maillard are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of sending a command to the tamper resistant module for renewing the encryption key periodically as described by Maillard with the method of monitoring the usage of service as taught by Andreaux because it would prevent the data from being reproduced *(Maillard, page 1, paragraph 9, lines 4 and 5)* and it would allow for subscriptions to a data access service *(Maillard, page 1, paragraph 11)*.

21. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Andreaux in view of Cutino et al. (EP 1263230 A1).

As per claim 4, Andreaux discloses: "Method according to claim 1," but fails to disclose expressly "characterized in that a command is sent to the tamper resistant module for Resetting/Updating the counter."

Cutino discloses "characterized in that a command is sent to the tamper resistant module for Resetting/Updating the counter." *(column 9, lines 4 through 8, counter is decremented per use, value can be added to card hence updating the counter)*

Andreaux and Cutino are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of updating the counter as described by Cutino with the smart card as taught by Andreaux because it is desirable to store monetary value on a card and later replenish it *(Cutino, column 9, lines 1 through 8).*

As per claim 5, Andreaux in view of Maillard disclose: "Method according to claim 3 or 4, characterized in that said command is encrypted by a third key (MK) known by the tamper resistant module." *(Maillard, page 4, paragraphs 58 and 59, additional key stored on smart card)*

Conclusion

22. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

23. The following reference teaches execution of trial data

US 2002/0174160 A1

US 2002/0159601 A1

US 1999/5892900

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571) 270-3906. The examiner can normally be reached on Monday to Friday 8:30 AM to 5:00 PM.

25. If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Thomas Pham, can be reached at the following telephone number: (571) 272-3689.

26. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

August 20, 2008

Simon Kanaan
Examiner
Art Unit 4148

SPK

/THOMAS PHAM/
Supervisory Patent Examiner, Art Unit 4148